دفاتر البحوث العلمية، المجلد 9، العدد 1، السنة 2021، الصفحة 259-279

الأبعاد الاستراتيجية للجرائم الإلكترونية وتهديداتها للأمن الوطني

Strategic dimensions of cyber crimes and its threats to national security

رياض بن عربية[1]

[1]المدرسة الوطنية العليا للصحافة وعلوم الاعلام، الجزائر، riadmag@yahoo.com

تاريخ الاستلام: 2021/04/28، **تاريخ القبول:** 2021/05/23، **تاريخ النشر:** 2021/06/08

الملخص: تستهدف هذه الدراسة عرض أهم الجوانب النظرية والتقنية المرتبطة بجرائم المعلومات بأبعادها وأشكالها المختلفة، باعتبارها من أخطر الأصناف المستجدة للجرائم والمستحدثة نسبيا في عصرنا الحالي، فهي نتاج وانعكاس للظواهر المرتبطة أساسا بالتطورات الحاصلة في ميدان تكنولو جيا الاعلام والاتصال أو ما يصطلح على تسميته "بالثورة الرقمية" أو "الموجة الثالثة". إلا أن المتتبع لهذا الشأن سرعان ما يلاحظ مدى التهديدات التي أضحت تمثلها تلك الجرائم الالكترونية سواء في حياة الأشخاص أو على أمن الدول ككل، جراء الانحرافات التي طالت استعمالاتها غير المشروعة من قبل قراصنة المعلومات أو الجناة الافتراضيين، هذه الظروف باتت تفرض نفسها بقوة خاصة مع بداية الألفية الثالثة، نظرا للخدمات والتسهيلات الكبيرة التي ما فتأت توفرها الطفرة التكنولوجية في هذا الجانب، لكن في مقابل تلك المزايا النسبية الظاهرة، هناك العديد من الآثار السلبية المسجلة خاصة تلك المتعلقة بالانكشافات والمخاطر المحتملة أو تلك الواقعة على الأمن القومي للدولةوعلى مؤسساتها الحكومية، مما بات الأمر يتطلب ضرورة تنسيق الجهود وتوحيد الرؤى وإيجاد الآليات القانونية والمادية المناسبة للحد من الجرائم الالكترونية، ومواجهة انعكاساتها المختلفة.

الكلمات المفتاحية: الجرائم الإلكترونية، الأمن الوطني، التهديدات، القراصنة المعلوماتيين، الثورة الرقمية.

Abstract: This study presents the most important theoretical and technical aspects of the different types of cybercrime. Cyber crime is one of the most dangerous emerging types of crime, reflecting developments in the field of information and communication technology or what is called the "digital revolution." The multifaceted threats posed by hackers against both individuals and states is very real, both in the lives of persons and on the security of States as a whole, as a result of the deviations that have been carried out on their illegal uses by hackers or virtual perpetrators, these circumstances have become particularly strong at the beginning of the third millennium, given the large services and facilities provided by the technological boom in this aspect, but in contrast to those apparent relative advantages, there are many negative effects recorded, particularly those related to exposures. The potential risks or those to the national security of the State and its

government institutions, which now require the need to coordinate efforts, unify visions, find appropriate legal and material mechanisms to reduce cybercrime and address its various repercussions.
Key words: Cyber crime, national security, threats, cyber hackers, digital revolutions.

مقدمة:

لقد مهدت الثورة الصناعية التي عرفتها البشرية في منتصف القرن 19 بروز ثورة جديدة ما إصطلح على تسميتها بثورة المعلومات والإتصالات، ولقد إتسمت هذه الثورة التي عرفتها خاصة مرحلة ما بعد الحداثة من ظهور جيل جديد من التطبيقات والبرمجيات التي شهدها قطاع الإعلام والإتصالوالرقمنة، حيث أفرزت هذه الأخيرة منظومة متطورة من البرامج الحاسوبية والشبكات الرقمية الناتجة عن التطورات الحاصلة والمتسارعة في مختلف الميادين، لاسيما تكنولوجيات وسائل الإعلام والإتصال والمعلومات.

وعليه، فلقد أدت هذه التحولات الناتجة عن الثورة الصناعية الثالثة(الثورة المعلوماتية)، والتي عززت القدرات والإمكانيات الهائلة التي أصبحت تشهدها الدول في العديد من المجالات، الأمر الذي انجر عنه بروز تحولات عميقة في بيئة المجتمعات والدول المستعملة لها، وظهور نمط جديد من الإستخدامات العلمية لهذه الوسائط التكنولوجيةالتي إجتاحت معظم دول العالم.

في هذا السياق، نجد أن هذه الثورة وبالرغم مما قدمته للإنسانية من تسهيلات عديدة ونافعة ، قلصت بموجبها الزمن ووفرت الجهد وسهلت من عملية الحصول على المعلومة في أي وقت وفي أي مكان، وذللت الصعاب التي كانت تواجها الشعوب والدول في هذا الخصوص، إلا أن هذه الثورة التكنولوجية وما أحدثته من نقلات وقفزات نوعية في مجال المعلومات والإتصالات، وتزايد الإعتماد عليهما في وقتنا الحاضر، سرعان ما قابله واقع جديد معاكس للإيجابيات التي حملتها هذه الأخيرة، حيث إتسم هذا الوضع الجديد الناشئ عن الإستعمالات المكثفة لهذه الوسائل الحديثة الرقمية، بضعف مستويات التجاوب والتعامل مع التهديدات الجديدة التي أفرزتها هذه الأخيرة بمختلف أبعادها وأشكالها، مما أدى بالعديد من الدول والمنظمات إلى ضرورة التفكير في إيجاد السبل الكفيلة لمجابهة الإنعكاسات السلبية والإستعمالات المضادة لمثل هذه الأساليب التكنلوجية خاصة من قبل شبكات الإجرام والتهريب والمافيا والقراصنة المعلوماتيين.

إنطلاقا مما سبق، وعلى ضوء الإفرازات الناشئة عن الإستخدامات المكثفة والمتسارعة للوسائل التكنولوجية الحديثة، يمكننا طرح الإشكالية التالية:**ما مدى مساهمة الجرائم الإلكترونية بمختلف أبعادها في تهديد الأمن الوطني للدول؟**

للإجابة على هذه الإشكالية المطروحة، إرتأيناإقتراح التصميم التالي لمعالجة الموضوع من مختلف جوانبه:

المحور الأول: الإطار المفاهيمي للجرائم الإلكترونية

قبل الشروع في تقديم المفاهيم المختلفة للجرائم الإلكترونية وضبطها وتحديدها بشكل عام، يمكننا القول أن العالم اليوم يعيش عصرا جديدا حسب المفكر الأمريكي ألفين توفلر(Alven TOVILR)صاحب كتاب الموجة الثالثة ،ألا وهو العصر المعلومات أو عصر ثورة المعلومات،التي أصبحت فيه صناعة المعلومات مصدرا للثروة ومقياسا لتقدم الأمم وأساسا للقوة الإقتصادية والسياسية والعسكرية. وقد نشأت هذه الثورة جراء تفاعل عاملين أساسيين: طفرة الإتصالات وطفرة تقنية المعلومات،فلقد حدثت طفرة في الإتصالات بموجبها تم تحويل العالم إلى قرية صغيرة، وربطت بين الشعوب المتباعدة، فأصبح الإنسان بمقدوره معرفة ما يجري في كل أنحاء الكرة الأرضية بمجرد الولوج في شبكة الأنترنت وبفضل خدمات الأقمار الصناعية، وأصبحت عملية تبادل المعلومات والمعارف على قدر من السهولة، حيث أدى إنتشار وسائل الإتصال المختلفة إلى تدفق هائل في المعلومات والأخبار والرسائل الثقافية[1]، لدرجة أن أطلق البعض على هذا العصر الذي نعيشه حاليا خاصة في السنوات 20 الماضية بقرن المعلوماتية "Le siècle de l'informatique".[2] من جانبه، فإن أنظمة المعلومات والشبكات ما فتأت في الآونة الأخير تحظى بأهمية بالغة في مختلف مناحي الحياة والمجالات، وأصبحت معها بذلك التكنولوجيات المعتمدة على الحاسب الآلي، البرمجيات وشبكات الاتصالات بمثابة الوسيلة الرئيسية والفعالة في نقل البيانات داخل مختلف منظومات الكيانات المؤسساتية، فضلا عن كونها المرتكز الاستراتيجي في مخططات البناء والتنمية[3]. ان هذا التطور الحاصل في مجال الثورة الرقمية والمعلوماتية بات يستلزم معه توفير الحماية اللازمة لهذه الأنظمة والبرامج التي تدخل في نطاق استخدامات شبكة الاتصالات والانترنت، على هذا النحو، بدأت التخوفات والتوجسات على أمن المعلومات والبيانات تأخذ منحى تصاعدي وتزداد حدتها يوما بعد يوم، مما استلزم معها وضع استراتيجية واضحة في هذا الشأن، تأخذ في الحسبان اتباع مجموعة من الإجراءات والقواعد والتشريعات التي يتم تنفيذها للحفاظ على سلامة وتكامل أنظمة المعلومات من التخريب والأعمال الهدامة ومختلف مظاهر الاستعمال غير المشروع لها[4]. بعد أن أعطينا لمحة وجيزة عن التطورات الحاصلة في مجال المعلومات وتقنيات الإتصال وما توفره من خدمات وتسهيلات عظيمة للأفراد، إلى جانب ما تحمله في مضامينها من مصادر تهديدات جمة جراء التصرفات المعادية الناجمة عن أفعال بعض الأفراد والشبكات المتآمرة المتنامية النشاط، والتي بات يتطلب الأمر لمواجهتها تسخير كافة الجهود والإمكانيات لمحاربة تلك الأنشطة التخريبية.فإننا سنحاول الإحاطة بموضوع الجرائم الإلكترونية.

الفرع الأول:مدخل تمهيدي حول الجرائم الإلكترونية

في السنوات الأخيرة ، أصبح البعض يطلق على الجرائم الإلكترونية بالجرائم المستحدثة، نظرا لأنها شكلت ثورة على نظم الجرائم المختلفة، فإذا كانت تقترب من الجريمة التقليدية من حيث الأركان العامة والخاصة، وتوفرها

على الفاعل والضحية وموضوع الجريمة، إلا أنها تختلف عنها من حيث صفات الفاعل ومميزاته، وطبيعة السلوك الإجرامي المنفرد بخاصية معنوية فريدة، ومسرح للجريمة ذي طابع معنوي، بالإضافة إلى تشعب وتنوع أصنافها وعدم قدرة النصوص الجزائية العقابية التقليدية على الإحاطة بهذه الصور الجديدة التي إبتكرها عقل الفاعل[5].

الأمر الذي إنجر عنه ظهور أزمة المصطلح، حيث ان المتتبع لظاهرة الجريمة المستحدثة التي أوجدتها ثورة الإتصالات وتقنية المعلومات عبر العالم، يجد نفسه أمام مشكل يتعلق بالمصطلح اللازم والكافي لوصف هذا النوع الجديد المستحدث من الجرائم. حيث إختلفت التسميات وتطورت معها الأوصاف التي لحقت بمثل هذه الجرائم، إلى درجة ان هناك من يطلق عليها جرائم إساءة إستخدام الكومبيوتر، جرائم إحتيال الكومبيوتر،الجريمة المعلوماتية، الجرائم المرتبطة بالكومبيوتر، جرائم التقنية العالية، جرائم القرصنة أو الهاكرز، الجرائم الإلكترونية[6].

ومع ظهور شبكة الأنترنت وإتساع تطبيقها دخل بعد جديد للإصطلاح السابق، فكانت التسمية تظهر بالإضافة إلى ما تم ذكره تسميات مختلفة: جرائم الكومبيوتر والإنترنت، جرائم الشبكة العنكبوتية، جرائم الأنترنت وجرائم الحاسب الآلي. وهناك من يسميها "بالجرائم ذوي الياقات البيضاء"[7]،للدلالة على أنها لا تحتاج إلى أدنى مجهود عضلي لارتكابها.الى جانب ذلك، فقد تعددت المصطلحات والمفاهيم المرتبطة بالجرائم الناشئة عن الاستخدام غير الشرعي لهذه الطفرة التكنولوجية والرقمية: الجريمة الالكترونية، الجريمة المعلوماتية، الغش المعلوماتي، جرائم التكنولوجيا، الجريمة الافتراضية والانحراف الافتراضي...، التي لا تعدو أن تكون مجموعة الجرائم المرتبطة بالأنظمة الالكترونية وشبكة المعلومات وعلى رأسها شبكة الأنترنت[8].

من خلال هذا التعريج البسيط على هذه الظاهرة، يتضح لنا جليا أن الأمر جد معقد من مجرد التسمية أو الأوصاف التي تطلق على مثل هذا النوع من الجرائم، القائم على وجود وتفاعل بين أشخاص مزودين بأجهزة الحاسب الآلي في علاقاتهم واتصالاتهم التقنية المرتكز على شبكة الإتصالات اللامحدودة، فالحاسب الآلي قائم على نظام معالجة آلية للمعلومات والبيانات، وأما الإتصال التقني فهو يساعد على توسيع الخدمة الممكنة ونقل وتبادل تلك المعلومات والبيانات بين أطرافالإتصال[9].

حتى أن الطابع القانوني لتكييف مثل هذه الجرائم الإلكترونية أصبح بالغ التعقيد والصعوبة في تعريف أركان تلك الجرائم نظرا لإتساع مدى ومحتوى الإستخدامات السلبية لأنظمة المعلومات وشبكات التواصل، بحيثإتسع نطاق ومفهوم الجريمة المستحدثة، فأصبح الحديث اليوم عن المجرم الإلكتروني أو المجرم المعلوماتي للدلالة على هذا النوع من الجرائم، فبات الحديث من قبل البعض على جرائم الكومبيوتر للدلالة على الجرائم التي يكون الحاسب الآلي محلا لها، فيما يرى آخرون أنها جرائم مرتبطة بالحاسب الآلي للدلالة على الجرائم التي تستخدم الحاسب الآلي وسيلة لإيقاعها[10].

بعد التطرقلأهم الجوانب المرتبطة بهذا النوع من الجرائم المستجدة، المتسم بتعدد التسميات وعدم ضبطه بصورة دقيقة ومحددة نظرا لتنوعها من جهة، فضلا عن صعوبة تكييف هذه الجرائم من الناحية القانونية وتميزها عنالجرائم التقليدية من حيث الوسائل والأطراف من جهة أخرى، فإننا سنحاول تقديم تعريفات ومفاهيم مختلفة لهذه الجرائم.

الفرع الثاني: المفاهيم المختلفة للجرائم الإلكترونية

من الأهمية بمكان أثناء دراستنا للجريمة الإلكترونية، أن نبدأ بعرض تعريف لها يحدد أبعادها ويشمل مجالاتها، ولكن قبل ذلك كان لزاما علينا أن نقدم تعريفا حول الجريمة بصفة عامة كمدخل لدراسة هذا الموضوع، في هذا الصدد، يمكننا القول بأن الجريمة هي أكبر صور العصيان على النظام الذي يكفله القانون، كما انها تمثل أبرز مظاهر التعدي على قواعد الإنضباط في المجتمع، وبالتالي فهي خروج على النظام الذي يضعه القانون.أما الجريمة كحقيقة قانونية فهي فعل ما يعاقب عليه المجتمع ممثلا في مشرعه، لما ينطوي عليه هذا الفعل من المساس بشرط يعده المجتمع من الشروط الأساسية لكيانه، أو من الظروف المكملة لهذهالشروط"[11].

لذا، فقد جرى تعرف الجريمة عموما في نطاق القانون الجنائي على أنها:" فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبيرا احترازيا"[12].فالجريمة اذن هي الفعل أو الترك الذي نص القانون عقوبة مقرره له،وبمقتضى ذلك لا يعتبر الفعل جريمة من الناحية القانونية إلا إذا كان ثمة نص على العقاب ولا عقاب من غير نص، إستنادا إلى القاعدة القانونية "لا جريمة ولا عقوبة إلا بنص"[13].

1-2 تعريف الجريمة الإلكتروني

إن الجريمة الإلكترونية مرتبطة إرتباطا وثيقا بالنظام المعلوماتي، بحيث نجد معاهدة بودابست لسنة 2001 بشأن مكافحة جرائم الفضاء المعلوماتي، التي قامت بتعريف النظام المعلوماتي بأنه " كل جهاز بمفرده أو مع غيره من الأجهزة من الآلات المتواصلة بينيا أو المتصلة، والتي يمكن أن يقوم واحدا منها أو أكثر تنفيذا لبرنامج معين بأداء المعالجة الآلية للبيانات"[14].

فالجرائم الإلكترونية هي صنف جديد من الجرائم، ذلك أنه مع ثورة المعلومات والإتصالات ظهر نوع جديد من المجرمين، إنتقل بالجريمة من صورها التقليدية إلى أخرى إلكترونية، قد يصعب التعامل معها نظرا لعدم وجود تعريف واحد موحد لها وهو ما يثير جملة من المشكلات العملية لمواجهتها وإيجاد الحلول اللازمة لها،إلا أنه تم تقديم مجموعة من التعريفات التي عالجت هذا النوع من الجرائم يمكننا سرد ما يلي[15]:

" كل فعل غير مشروع يكون العلم بتكنولوجيا الكومبيوتر بقدر كبير لازما لإرتكابه من ناحية وملاحقته من ناحية أخرى"." هي تلك الجرائم التي تقع على جهاز الكومبيوتر أو داخل نظامه فقط". أو هي" الجرائم الإلكترونية هي كل الجرائم التي تتم في محيط أجهزة الكومبيوتر". "هي كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها". جرى تعريفها كذلك على أنها "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول للمعلومات المخزنة داخل الحاسب أو تلك التي يتم تحويلها عن طريقه"[16].هي "كل نشاط وعمل اجرامي تم تنفيذه في الفضاء الرقمي عن طريق شبكة الأنترنت، شبكات الهاتف أو بطاقات الشرائح الذكية، باستخدام مختلف صور وأشكال البرامج الخبيثة التي ساعد على ارتكابهاالاستفادة من مزايا ثورة تكنلوجيا المعلومات والاتصالات[17]. كما ذهبت بعض الدراسات العلمية إلى تعريفها على" أنها الجرائم المرتبطة بالكومبيوتر، والتي تمثل إنتهاكا للقانون الجنائي، ويستوجب إرتكابها أو التحقيق فيها أو المحاكمة بشأنها دراية بالأمور الفنية للكومبيوتر"[18]. من جانبه، فقدعرفها البعض على أنها" نشاط غير مشروع، موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب، أو التي تحول عن طريقه".اتجه الفقيه MASSالى تعريفها على أنها " تلك الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بهدف تحقيق الربح"[19].

أما الفقيهان CREDO &MICHEL فقد اعتبرا أن سوء إستخدام الحاسب أو جريمة الحاسب تشمل:إستخدام الحاسب كأداة لإرتكاب الجريمة، هذا بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه، أو بياناته، كما تمتد جريمة الحاسب لتشمل الإعتداءات المادية سواء على جهاز الحاسب ذاته أو المعدات المتصلة به، وكذلك الإستخدام غير المشروع لبطاقات الإئتمان، وإنتهاك ماكينات الحساب الآلية، بما تتضمنه من شبكات تحويل الحسابات الماليةبطرق إلكترونية، وتزييف المكونات المادية والمعنوية للحاسب، بل وسرقة جهاز الحاسب في حد ذاته أو أي مكون من مكوناته"[20]. ان منظمة التعاون والتنمية الاقتصادية (OCDE) اعتمدت مفهوم الجرائم الالكترونية للدلالة على" على كل تصرف غير مشروع أو منافي للأخلاقيات أو غير مسموح، والمتعلق أساسا بالمعالجة الآلية للمعطيات أو نقل البيانات" [21].في حين عرفتها منظمة الأمم المتحدة على أنها " جريمة يمكن إرتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوبي، وتشمل تلك الجريمة جميع أنواع الجرائم التي يمكن إرتكابها في بيئة إلكترونية"[22].

2-2 تعريف المجرم الالكتروني أو المعلوماتي:

لتحديد المجرم الالكتروني ينبغي أولا الوقوف على أهم ملامح صفاته، لذلك فهو بوجه عام[23]:

- مجرم متخصص يتمتع بقدرات جد فائقة من حيث المهارات التقنية التي يستخدمها لتنفيذ مخططاته الاجرامية (اختراق الشبكات، كلمات المرور وفك رموز التشفير).

- يتمتع بدرجة عالية من الحضور الافتراضي والغوص في الفضاء الرقمي التي تسمح له بالاطلاع البيانات والمعطيات المتوافرة في الشبكة، لتحقيق مخططاته الاجرامية.

- تواتره على ارتكاب الجرم، فهو عائد ومتعود دوما على مثل هذه الجرائم، حتى أنه قد لا يحقق الاختراق بهدف الايذاء وانما نتيجة احساسه الكبير بالتفوق وقدرته اللامتناهية على الاختراق.

- مجرم محترف هدفه الثراء وتحقيق الكسب: يتمتع بقدر عالي من الذكاء الذي يؤهله لتنفيذ هجمات الكترونية من شأنها احداث الضرر بمصالح الغير (السرقة والنصب الالكترونيين، الاعتداء على حقوق الملكية الفكرية مقابل المال).

2-3 أسباب انتشار الجريمة الالكترونية

مما لا شك فيه أن الجرائم الالكترونية بمختلف أبعادها تختلف اختلافا كبيرا عن الجرائم التقليدية العادية، سواء من حيث المحل أو الخصائص -كما سنبين ذلك لاحقا-على هذا الأساس، فإن الأسباب والدوافع المؤدية لارتكابها تختلف هي الأخرى في جوهرها ومضمونها عن باقي الجرائم الأخرى، ومن بين هذه الأسباب يمكن ذكر ما يلي[24]:

- الرغبة في التعلم والاستكشاف من خلال التحكم في تقنيات الكومبيوتر وأنظمة المعلومات.
- الميل نحو تحقيق الثراء والربح السريع وتعظيم المكاسب المادية بطريقة سهلة من قبل هؤلاء المجرمين.
- حب المغامرة والانبهار بالتقنية العالية وتحقيق المتعة الشخصية.
- المؤثرات السيكولوجية والميول الشخصية والنزوع نحو الفردانية لتأكيد الذات.

2-4 خصائص الجرائم الإلكترونية

من خلال سرد التعريفات السابقة للجرائم الإلكترونية وتحديد دوافعها، يمكننا إستخلاص أن لهذه الجرائم سمات معينة تختلف عن الجرائم التقليدية الأخرى،بإعتبارها إفراز ونتاج لتقنية المعلومات، وإتساع نطاق تطبيقها في المجتمع، مما يعطيها طابعا قانونيا خاصا بها، ويميزها بمجموعة مشتركة من الخصائص، بحكم أن الاجرام في الفضاء السيبرياني[25]*مرتبط الى حد بعيد بأنظمة الشبكات وبدرجة المستخدمين لها.

ومن بين أبرز الخصائص التي تميز الجرائم الالكترونية عن غيرها من الجرائم التقليدية نجد[26]:

1- جرائم مغرية للمجرمين وسهلة الإرتكاب: فهي إذن سريعة التنفيذ لا تقتضي التواجد في مسرح الجريمة.

2- الجريمة الإلكترونية هي جريمة عابرة للحدود: اي أنها تتسم عادة بالطابع الدولي، نظرا لإتصالها بشبكات الحاسب الآلي مما يسهل إرتكابها من دولة إلى أخرى. فهي جريمة عابرة للقارات.

3- جرائم صعبة الإثبات: فهي تتصف دائما بالضبابية، أي عدم وجود آثار مادية يمكن متابعتها وملاحقة مرتكبيها، فهي صعبة الإكتشاف، ويصعب تحديد مكان وقوعها أو مكان التعامل معها، بمعنى عدم تركهالأي آثار لها بعد إرتكابها.

4- عدم وجود مفهوم مشترك للجريمة المعلوماتية: ويظهر هذا جليا في عدم وجود تعريف قانوني موحد لها.هذا بالرغم من الجهود الدولية المبذولة في هذا الشان (إتفاقية بودابست لسنة 2001).

5- وقوع الجريمة المعلوماتية أثناء المعالجة الآلية للبيانات: فهي تقع أثناء عملية المعالجة الآلية للبياناتوالمعطيات الخاصة بالكومبيوتر، وهو ما يمثل الشرط الأساسي لقيام أو عدم قيام أركان الجريمة المعلوماتية.

6- قلة الإبلاغ عن وقوع الجريمة المعلوماتية: نظرا لعدم إكتشاف الضحية لها أو لخشيته من التشهير، فعادة ما يتم إكتشافها عن طريق المصادفة، فالعديد من الجرائم التي لم تكتشف هي أكثر بكثير من الجرائم المكتشف عنها.

7- ارتكابها في الخفاء: حيث أن عملية نقل البيانات والمعطيات تكون منحصرة أساسا في شكل نبضات إلكترونية[27]

8- اتساع نطاق أضرارها فهي اذن جريمة مخلفة لخسائر فادحة نظرا للآثار المترتبة عليها[28].

9- هي جرائم سهلة الارتكاب بعيدا عن الرقابة الأمنية لأن مرتكبيها يصعب التنبؤ بهم أو الإيقاع بهم بسهولة، نظرا لقدرة الجناة على اتلاف الأدلة والوثائق من مسرح الجريمة[29].

المحور الثاني:الأبعاد المختلفة للجرائم الإلكترونية

لا يخلو نطاق ثورة المعلومات وتكنولوجيا الاتصال من العديد من المظاهر السلبية المصاحبة لها، خاصة لما يتعلق الأمر بالاستخدام غير المشروع من قبل الجناة والمجرمين لتحقيق مآربهم وأهدافهم الشخصية. فهذه الموجة السريعة للابتكارات التي يسميها البعض "تيكنامي" (Technami) تيمنا بحادثة تسونامي، جلبت معها موجة من التهديدات المؤثرة وسلسلة من الآثار الجانبية الواقعة على أمن المعلومات، التي أضحت مدعاة للقلق[30].

نتاجا لذلك،فقد شهد أواخر القرن الماضي إزدياداً هائلا في حقل الجرائم الإلكترونية وتغييرا في نطاقها ومفهومها، وكان هذا بفعل ما أحدثته شبكة الأنترنت من تسهيلات عديدة لعمليات دخول وإقتحام شبكات المعلومات، فظهرت أنماطا جديدة من هذه الجرائم السيبريانية، التي إتخذت مظاهر مختلفة وأصبحت تطرح اليوم إشكاليات خطيرة على الأصعدة الاستراتيجية، الأمنية، القانونية والإقتصادية.

وعليه، سنحاول إعطاء بعض النماذج عن الجرائم الإلكترونية التي باتت وتيرتها في تصاعد متزايد ونشاطاتها تعرف دينامية أكثر من أي وقت مضى، بسبب التطورات المتلاحقة التي تعرفها ثورة المعلومات والإتصالات، وهذا من خلال تعرضنا لشكلين رئيسيين من الجرائم الإلكترونية، الذين يحويان بداخلهما العديد من أشكال الجرائم المعلوماتية.

الفرع الأول:الجرائم التقنية ذات الصبغة المالية[31]:

1- جرائم الإتلاف التقني:

يمثل حق الملكية حق رعته مختلف القوانين والتشريعات سواء من الناحية المدنية او الجزائية، وهو ما نجده جليا في قانون العقوبات الذي يحتوي على العديد من النصوص الجزائية التي جرمت كافة أشكال الإعتداء على حق الملكية، وإمكانية الإستئثار بالشيء من قبل صاحبه.وأمام هذا الوضع المقلق اهتم المجتمع الدولي بمسألة مكافحة الجريمة المعلوماتية، وفي هذا الصدد نشير إلى أن منظمة الأمم المتحدة قد أولت مسألة مواجهة الجرائم المعلوماتية اهتماما كبيراً خصوصا خلال مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين الذي انعقد في فيينا أيام 10 – 17 ابريل 2000، وكذلك خلال مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية الذي انعقد في بانكوك أيام 18-25 ابريل 2005.

2- جرائم السرقة التقنية:

لقد إعترفت معظم التشريعات بحق الملكية وصيانتها وهو ما يمثل الضمانة والأساس القانوني الذي إنطلقت منه الحماية الجزائية لهذا الحق، وهي ظاهرة في تجريم كل أشكال الإستلاء على المال وحرمان صاحبه منه، بأية وسيلة كانت بدون علمه أو بدون رضاه.هذه الحماية هي مكرسة بموجب قانون ثابت يحمي حق الملكية، هذا الحق الثابت بموجب سند القانون، فكان حق الملكية محلا لعدد لا حصر له من الإعتداءات، ومن أبرز هذه الإعتداءات على حق الملكيةهو الإعتداء بالسرقة، من خلال نزع المال من ملك صاحبه وحرمانه منه بصفة دائمة[32]. ففي سنة 2014 إعترف البنك الأمريكي " J P Morgan" بأن حوالي 76 مليون شخص من زبائنه وحوالي 7 ملايين مؤسسة صغيرة ومتوسطة تعرضت لعمليات القرصنة [33].

ومع تطور نظم المعلومات وتعديل مفهوم المال، إتسعت سلوكيات الأفراد وتطورت أساليبهم في تحقيق الإستلاء على أموال الأفراد بمساعدة وسائل التكنولوجيا وأنظمة الحواسيب الإلكترونية.حيث تشير بعضتقارير المصالح الأمنية في الولايات المتحدة الأمريكية إلى أن 500 مليون دولار أمريكي سنويا يتم سلبها من أصحاب البطاقات الائتمانية أو جراء الإستلاء على حسابات الأشخاص بواسطة المعلومات [34].

3- جريمة التزوير المعلوماتي التقني:

ان تزوير البطاقات النقدية عبر مختلف التعاملات المالية يعتبر أحد المظاهر الرئيسية الكبرى للجرائم الالكترونية، أين نجد أن سرقة البيانات الشخصية للأفراد على النت والتلاعب بها أضحى أحد الهواجس التي تؤرق بال المواطنين وتفقد ثقتهم في الدولة، خاصة وأن التأسيسلهذه الثقة هي بمثابة أكبر رهان لانتعاش ونمو الاقتصاد الافتراضي في المستقبل[35].

تمثل جرائم التزوير بمختلف أنواعها من العقوبات التي تعاقب عليها مختلف التشريعات والنصوص القانونية والجزائية في معظم بلدان العالم، وهذا بالرغم مما يتوافر بين السلوك التقليدي للتزوير والسلوك المستحدث من تشابه من حيث الأضرار والنتيجة، وتكمن خطورة هذه الأعمال الإجرامية نظرا لما تلحقه من أضرار مادية تقع على تقنية نظم المعلومات في العمل الحكومي والأعمال الخاصة ، مما يعظم الحاجة لحفظ هذا السلوك المستحدث في قالب تجريمي لملاحقة الفاعل جزائيا، جراء تلاعبه بالمحررات الإلكترونية الرسمية والشخصية وما قد ينجر عنه من إنعكاسات خطيرة على حياة الفرد والدولة على حد سواء[36].

4- جرائم غسل الأموال التقنية:

تعد أفعال غسيل الأموال بكافة أشكالها من الجرائم ذات الخطورة العظيمة والمضاعفة، فهي تبنى على مخالفات جرائم إرتكبت أصلا، تحصلت فيها أموالا قذرة أو مشبوهة. ثم هي من جانب آخر تدخل هذه المتحصلات الماليةفي أنشطة إجرامية أخرى، كتمويل الإرهاب والعمليات غير المشروعة، مما أمكن وصف جريمة غسل الأموال بأنها جريمة بين جرائم، فهي تبنى على مخلفات جريمة سابقة أو جرائم سابقة، ثم تقع هي كحلقة لسلسلة الإجرام . إذ تعتبر هذه الجريمة تمويلا أو تمهيدا لجرائم أخرى تعد أكبر خطو رة من الأولى. هذه الخطورة وما يصاحبها من أضرار طائلة على الإقتصاد وأمن الدولة وعلى الصعيدين المحلي والدولي، دفع بالجهود الدولية والوطنية نحو سن تشريعات وقوانين وأنظمة وتعليمات كفيلة بضبط هذه الجرائم وتحديد أصول التحقيق فيها، وملاحقة الجناة، ثم أسس وأصول التعامل مع متحصلاتها من أموال غير مشروعة وتشكيل توافق مع طبيعة هذه الجرائم خصوصا بشكلها الإلكتروني، إذ ان هناك توافقا وإرتباطا بين السلوك الإجرامي في جرائم غسل الأموال بالبيئة الإلكترونية التي توفر الأرضية الخصبة لجميع النشاطات المشبوهة[37].

5- جرائم البطاقات المالية:

في إطار ثورة تقنية نظم المعلومات بدأت المجتمعات تبتعد شيئا فشيئا عن الإستخدام التقليدي للنقود ، وحصرت إستخدام الأوراق التجارية في بعض الأعمال، حيث مع ظهور النقد الإلكتروني تم اللجوء إلى إستخدام البطاقات المالية بمختلف صورها، و في المجالات المخصصة لها (بطاقات الإئتمان، أو بطاقات الصراف الآلي،

البطاقات الذكية) وبالرغم من المزايا التي تحققها هذه البطاقات والتكنولوجية والتقنية العالية المعدة لإستخدامها وبرامج الحماية المصممة لها، إلا أن الجانب الإجرامي لدى البعض عمل على إختراقها وإساءة إستخدامها، بحيث يتم الإعتداء عليها بصورة تلحق العديد من الأضرار على مستعمليها ومالكيها الشرعيين[38] وبين المتعاملين بها، وهو ما يؤدي في كثير من الحالات إلى وقوع السرقات المادية والإستلاء على الأرصدة المالية المخصصة لأصاحبها الحقيقيين.

6- جرائم تزييف العملات:

لقد سعى الانسان منذ القديم في اطار صراعه مع الطبيعة ومع غيره من البشر الى محاولة فرض ارادته وتغليب مصلحته على حساب مصالح الآخرين ولو بطريقة غير مشروعة، فلما عرف الانسان النقود والعملات تبادرت لديه فكرة تزوير العملات وتزييفها لتحقيق مطامعه الشخصية في الربح غير المشروع، وتنعكس خطورة هذه الجرائم من حيث انعكاساتها على أمن الدول والمجتمعات على حدة سواء، جراء ما تخلفه من اضطرابات واضرار بالمصالح العامة للدولة والخاصة للأفراد، وكذا آثارها البليغة على النظم الاقتصادية والمالية للأمم، ومما سهل عملية رواجها على نطاق واسع، هو سهولة ارتكباها وتحولها من جرائم عنف الى جرائم احتيال، انتشار التقنيات الحديثة المساعدة على ذلك، فضلا عن كونها جريمة عابرة للحدود والأوطان ومتعددة الجوانب[39].

الفرع الثاني: جرائم تقنية الإتصالات المعلوماتية

مع تعميم الإستخدامات الحديثة القائمة على الوسائط التكنولوجية الجديدة البعدية والقدرة على إجراء إتصالات بين نهايات طرفية لا محدودة، ووجود القدرة على الإتصال بهوية مصطنعة، كل ذلك أدى بالسلوك الإجرامي في المجال التقني إلى القيام بأنشطة وأعمال تخريبية تستهدف العديد من الأشخاص والدول والمنظمات، بفعل التقنية العالية على الإيقاع بالضحايا وإخفاء الهوية الحقيقية للفاعل.فلقد مهدت شبكات الأنترنت والإتصالات العالية التدفق الطريق أمام إجرام من نوع جديد وبأساليب جد متطورة تعقد من مهمة التعرف على الفعل وتحديد هوية الفاعلين، ثم ظهر مصطلحcybercrime الذي يعني الجرائم التي تستخدم بإستعمال جهاز الحاسب وشبكة الأنترنت، أين وصل الأمر ببعض الدول إلى إطلاق مبادرة حماية المجال المعلوماتي cyberspace كما فعلته الولايات المتحدة الأمريكية سنة 2003[40].

وعليه، يمكننا تتبع أهمأنواع هذه الجرائم ذات الصلة باستخدامات تقنية الإتصالات المعلوماتية، من خلال التعرض إلى[41]:

1- جرائم الإعتداء على الحياة الخاصة للأفراد:

أدى ظهور خدمات الحاسب الآلي الآخذفي التطور بسرعة مذهلة إلى أن أصبح يمثل السمة الرئيسية لعصرنا الحالي، نظرا لما يحتويه من قدرات وإمكانات هائلة في تنفيذ المهام والقيام بأعمال يعجز عنها الإنسان بحد ذاته، وهو ما زاد من درجة الإعتماد والترابط الوثيق بين الإنسان والحاسب في جميع مناحي الحياة اليومية والمهنية للأفراد، بحيث إعتمدت مختلف نشاطات البشر عليه بالتخزين والمعالجة والإسترجاع لمختلف البيانات والمعطيات الخاصة والشخصية التي يحتويها هذا الحاسب،بحيث أصبحت الحياة الخاصة للإنسان جزءا من هذا النظام، وعليه فإن درجة إختراق أو الإستلاء على هذه المعطيات الشخصية أصبح أكثر سهولة من أي وقت مضى، خاصة إذا علمنا أنه في سنة 2011 يوجد أكثر من 2.3 مليار شخص مرتبط بشبكة الأنترنت وهو ما يمثل ثلث سكان العالم[42]،نظرا توفره هذه التكنولوجيا الرقمية الحديثة من ميزات تسهيلية تساعد على الولوج لمثل هذه القاعدة من البيانات الشخصية.

وهو مازاد من حدة تعرض حياة لأفراد الشخصية لعمليات قرصنة جراء السعة التخزينية الضخمة لأجهزة الحاسب الآلي، ثم السعة اللامتناهية لشبكة الربط المعلوماتيالعالمية، بالإضافة إلى إمكانية التحقق الربط البعدي لجهاز الحاسب الآلي مع أكثر من جهاز عبر العالم، وهذا في ظل قدرة العقل على إختراق نظم الإتصالات بطريقة أو بأخرى والوصول إلى مكان تواجد المعلومات والبيانات ذات العلاقة بالحياة الخاصة بالأفراد.

2- جرائم الإنترنت المتعلقة بالقاصرين:

بفضل ما توفره من مزايا المتعة والتفاعلية في يوميات القصر والمراهقين، أصبحت الأنترنت والوسائل التكنولوجية الحديثة تشكل خطرا على حياة هؤلاء القصر (حوالي 7.5 مليون) التي هي في ازدياد مطرد، ومن منطلق أنها تشكل أهداف تجارية بالدرجة الأولى لقد إمتدت الأعمال الإجراميةالإلكترونية والأنشطة المعادية لتطال فئة عمرية تحظى أصلا بالحماية والرعاية الخاصة، فلقد أصبح ضحاياها القاصرون موضوع اعتداءات متكررة، آخذة في الإتساع، سواء تعلق الأمر بالمواد الإباحية للأطفال أو المواضيع المفسدة للأخلاق، ففي فرنسا مثلا، تمثل نسبة الجرائم المرتبطة بالاعتداء الجنسي على الأطفال ما بين 20% و40% من القضايا المعالجة كل شهر[43].

في هذا السياق، يمكننا رصد بعض صور الإعتداءات الجرمية الواقعة على القاصرين بمناسبة إستخداماتهم لهذه الوسائط:

- ✓ تحريض القاصرين على الأعمال الجنسية
- ✓ إنتاج صور فاضحة للقاصرين

- ✓ إستغلال الأطفال القاصرين جنسيا
- ✓ تشجيع القاصرين على نشاط الدعارة والأعمال الإيباحية

3- جرائم أعمال الدعارة والترويج لها

وهي تلك الجرائم التي تروج عبر شبكات الإعلام الآلي والتواصل الإجتماعي لأعمال ونشاطات تمس بعادات وتقليد المجتمعات وتضر بآدابها، وهذا من خلال تشجيعها لممارسات الدعارة عبر إستغلال شبكات المتجارة بالرق الأبيض أو إنتاجها لصور أفلام إيباحية والترويج لها عبر هذه التقنيات الجديدة للتواصل، وبالتالي القيام بأعمال جنسية مختلفة تساهم في إفساد أخلاقيات وسلوكيات الأفراد.

4- جريمة التجسس الإلكتروني:

يعرف سلوك التجسس بأنه كل فعل قوامه الكشف وإستظهار الحقائق المخفية بطرقة غير مشروعة، أو بوسائل أو غايات غير مشروعة، وهو ما يتوجب عليه عقوبة جزائية ردعية لمعاقبة هذه التصرفات والأفعال المضرة بأمن وسلامة البلد، سواء كانت هذه السلوكات تخص معلومات شفهية أو كتابية أي كان نوعها، طالما أنها تتسم بطابع السرية والكتمان، التي لا يجوز الإطلاع عليها أو كشف مضمونها.

ويتعلق الأمر هنا فيما يخص جرائم التجسس الإلكتروني:

- ➢ أسرار وثائق الدولة: وهي تلك الوثائق الرسمية التي اهتمت الدولة بها منذ نشأتها وعملت على حفظها وحمايتها، خاصة تلك المعلومات المتعلقة بكيانها أو نشاطها او مخططاتها الإستراتيجية،
- ➢ الأسرار والوثائق الخاصة: وهي جميع الوثائق والمعطيات والأسرار والمعلومات ذات الطابع الشخصي والمصلحي.

5- جرائم الإرهاب الإلكتروني:

عموما، فإن الإرهاب الالكتروني بالمعنى الدقيق للكلمة ليس ظاهرة جديدة وليدة اللحظة، ولكن الهجمات الالكتروني التي ينفذها القراصنة المخترقون هي التي تضاعفت حدتها في السنوات الأخيرة من خلال أعمال التشويه، التشبع والانتحال التي تطال المواقع الالكترونية، نشر الفيروسات[44].

ومنه، فظاهرة الإرهاب قديمة متجددة لم يسلم منها مجتمع من المجتمعات على مر العصور، مع إختلاف صورها وأنواعها ودرجاتها،حيث إستغلت الكثير من الجماعات المتطرفة الطبيعة الإتصالية للأنترنت من أجل بث معتقاداتها وأفكارها، بل تعداه الأمر إلى ممارسات أصبحت تهدد أمن الدولة المعتدي عليها، خاصة الإرهاب والجريمة المنظمة، اللذان أخذا منحى آخر في إستعمال الأنترنت، الأمر الذي سمح لهم بإرتكاب جرائم غاية في

الفتك في حق الشعوب والدول[45].ويعتبر الإرهاب في ظل الظروف الراهنة بديلا عن الحروب التقليدية، فهو إذن إستراتجية عنف منظمة تمارس من قبل شخص، تنظيم، دولة، جماعة...، مع إستعمال وسائل التهديد، من أجل خلق حالة من الرعب والذعر لتحقيق أغراض ومكاسب سياسية[46].

أين كانت غاية الفاعل والمساهمين معه في جرائم الإرهاب وعلى الدوام إيقاع الضرر بآمن المجتمع ومقدرات أفراده، وزعزعة امن وإستقراره،أما الوسائل المعتمدة في ذلك من قبل الفاعل فقد بدأت تقليدية بحتة إعتمدت على الحركة والقوة والعنف ثم ما فتأت بفعل تطور نظم الإتصالات المعلوماتي وإنتشار وسائلها وشيوع شبكات الأنترنت أن أخذت منحى آخر يعتمد بالدرجة الأولى على تقنيات هذه التكنولوجيا في إيقاع الأضرار وإستهداف أمن وسلامة المجتمعات والدول، فظهر مصطلح جديد يعرف بالإرهاب الإلكتروني CYBERTERRORISM، حيث يستفيد الفاعل والمساهمون معه من تقنيات عالية النفاذ لتحقيق أهدافهم.

فالإرهاب الإلكتروني كمصطلح مستحدث لا يزال يكتنفه الغموض، نظرا لإعتماده على تقنية أنظمة المعلومات من حيث وسيلة إرتكابه، ومن حيث دور الفاعل فيهوطبيعة سلوكه، وهدفه هو تحقيق إيقاع الرعب لدى الناس وترهيب حياة الأشخاص والحكومات وتعريضها للخطر.أما خطورة الإرهاب الإلكتروني فتتعاظم في حالة مدى إتساعإعتماد المجتمعات على تقنية أنظمة المعلومات سواء في نطاق الدولة الواحدة أو في نطاق إقليمي عالمي، في مقابل إنعدام البيئة التشريعية اللازمة لمكافحة جرائم الإرهاب الإلكتروني على وجه الخصوص.

المحور الثالث: الجرائم الإلكترونية وتهديدها للأمن الوطني

بعد أن معالجتنا في المحورين الأولين لماهية الجرائم الإلكترونية وأبعادها المختلفة، سنحاول في هذا المحور معالجة التهديدات المختلفة للجرائم الإلكترونية للأمن الوطني، بإعتبارهيمثل أهم غاية تحاول كل دولة تحقيقه.

أصبح من السهولة بمكان في وقتنا الحالي في ظل التطورات المتسارعة لتكنولوجيات الاعلام والاتصال والرقمنة ارتكاب أخطر أنواع الجرائم المعلوماتية في حق الأفراد أو المؤسسات أو الدول، نظرا لاعتمادهم الكبير على شبكات الأنترنيت. لذلك، فالجريمة الالكترونية تعتبر من الأشكال الجديدة للجرائم العابرة للقوميات والحدود الوطنية، مما حدا بكثير من المنظمات والهيئات الدولية الى اعلان خطورة تلك الجرائم التي تستهدف رواد الشبكة العنكبوتية على المستوى الدولي[47]. فعادة ما تسعى الدول إلى حماية أمنها الوطني، الذي يمثل هدف الدول المنشود المتمثل في خلق الظروف التي يمكن أن يصل فيها أفراد شعبها الحد الأقصى لإشباع حاجاتهم ،حيث تتحدد وظيفة الدولة في حماية الإستقلال وحفظ الأمن الداخلي، وتلبية حاجيات الشعب وتحقيق رفاهيته من خلال

ممارسة نشاطاتها المختلفة السياسية، الإقتصاديةوالإجتماعية والعسكرية التي تعبر في الوقت نفسه عن المظهر المادي للسلوك الوظيفي للدولة، لأن أي إضرار بأحد أنشطة الدولة ينعكس عليها وعلى أفرادها بالضرورة، وهو ما عبر عنه وزير الخارجية الأمريكي الأسبق **هنري كيسنجر** "بأن الأمن القومي هو أي تصرفات يسعى المجتمع من خلالها إلى تأكيد حقه في البقاء"[48]. فإذا كان الأمن القومي بوجه عام يهدف إلى حماية كيان الدولة ضد كافة أشكال العدوان، فإن الأمن المعلوماتي يشير إلى تلك الجهود الرامية إلى حماية موارد المعلومات المنظمة من سوء الإستخدام من قبل الأطراف غير المصرح لهم من خلال تحديد التهديدات التي قد تواجه أمن المعلمات وتشخيص نقاط الضعف التي يعاني منها برنامج امن المعلومات ومن ثمة تحديد المخاطر المترتبة على تلك التهديدات وإستغلال نقاط الضعف، ووضع سياسة أمن المعلومات وتنفيذ الضوابط والمعايير التي تساهم في تعزيز أمن المعلومات[49]. هذا ما يدفعنا للقول بأن تلك الجرائم الإلكترونية بصورها المختلفة تمثل أحد أهم العناصر المهددة لكيان الدولة وزعزعة أمنها وإستقرارها عبر مختلف الأنشطة والأعمال التخريبية المعادية التي تستهدف أجهزة ومؤسسات الدولة وأنظمة معلوماتها الحساسة، من خلال محاولة التأثير على تلك البرامج وتخريبها حتى تتعطل مختلف نشطات وأجهزة الدولة الحاسة مما يخلق حالة من الفوضى والإضطراب التي قد تصيب أجهزة العصبية الرئيسية في الدولة وتعمل على شللها وإضعافها. على هذا النحو، هناك العديد من التهديدات والمخاطر المحتملة الواقعة على أنظمة المعلومات وبصورة خاصة أمن المعلومات، سواء تعلق الأمر بتلك المرتبطة بالداخل أو حتى احتمالية الاختراقات التي يكون مصدرها خارجي، مما يؤدي في نهاية المطاف الى اختراق حسابات وبيانات الأشخاص والكيانات الكترونيا بطريقة غير شرعي، نظرا للثغرات الأمنية المصاحبة لتلك القواعد البيانية والقصور في إجراءات الحماية[50]. فالدولة عادة ما تحرص على إتخاذ كافة التدابير الملائمة لغرض الحفاظ على وضع الأمور مقابل المستوى المطلوب من الأمن، وخاصة، حماية الحقوق المتصلة بالأصول والموجودات المعلوماتية، التي تتكون من البيانات الخام التي نظمت في صيغة وثائق والوسائط والحقوق المتعلقة بإستخدام المحتويات الفعلية[51].

ومن بين التهديدات التي قد تتعرض لها الدولة ومؤسساتها بفعل تلك الجرائم الإلكترونية يمكن ذكر ما يلي[52]:

- الاختراقات التي تصيب الأنظمة الحكومية بما فيها أنظمة التحكم المسؤولة عن المنشآت الحساسة (لقد تعرضت الحكومة الكندية في جويلية 2007 الى هجمة إلكترونية مكثفة شلت مختلف قطاعاتها الوزارية).
- الحرب الالكترونية.
- الجرائم الإلكترونية الإرهابية.

-إختراق أمن معلومات الدول إلى الحد الذي قد يتعذر معه أحيانا الكشف عن الجهة الحقيقية التي تقف وراء تلك الإختراقات، مما يرهن كافة النشاطات والخدمات والأعمال الرسمية التي تمارسها أجهزتها المختلفة.

- إصابة وشل البنية التحتية الحرجة في الدولة بفعل الإختراقات المتكررة، التي تشمل النظم والشبكات المترابطة التي يكون له تأثير خطير على الصحة، السلامة، الأمن أو حتى الرفاه الإقتصادي للمواطنين، أو على الأداء الفعال للحكومة في ضمان إستمرارية النشاط الرسمي للدولة من ضمان الخدمات المصرفية، الإتصالات السلكية واللاسلكية، التعرض لخطوط التدفقات العالية للأنترنت... ، بحيث نجد أن هذه الهجمات على البنى التحتية الحرجة أصبحت أكثر تعقيدا من أي وقت مضى نظرا لسهولة إحداث الأضرار بتلك البنى، وعلى سبيل المثال فقد تعرضت إيران في سنة 2010 إلى هجمات إلكترونية أصابت مرفق معالجة تخصيب اليورانيوم، بحيث تم وصف الخبراء البرمجيون ذلك الهجوم على أنه صاروخ أرض أرض إلكتروني عسكري[53].

- الهجمات على مرافق الأمن والدفاع الوطني التي تعتبر مرافق جد حساسة وحيوية نظرا لإتصالها بالوجود الأساسي للدولة وحمابة كيانها من مختلف أشكال الإختراق، فأصبح الحديث اليوم عن هجمات الجيوش الإلكترونية النشطة في العديد من الدول، وإمكانياتها على إصابة القدرات الدافعية والهجومية للدول.

- إرتفاع معدلات القرصنة التي تتعرض لها الأجهزة الحكومية في الدولة، فإذا كانت القرصنة هي التعدي على حقوق الآخرين بصورة غير مشروعة ولا أخلاقية في مجال الكوميوتر، والتي قد تأخذ عدة أشكال:القيام بسنخ برامج الغير إما بغرض الإستعما أو البيع، إختراق الشبكات وتدمير أنظمتها بدافع الإنتقام أو الإختلاس، إختراقأنظمة البنوك والشركات الكبيرة والتلاعب ببياناتها مما يكبدها خسائر هائلة[54].

كذلك، فإن من بين أخطر مما تتعرض له الدولة في إطار الجرائم الإلكترونية، هو القدرة الفائقة والعالية للتجنيد والتعبئة التي تتمتع بها شبكات الإجرامية التخريبية، وذلك من خلال إستغلالها لتلك التكنولوجيا المتطورة لدعم الإرهاب والتطرف، أو محاولة نشر أفكارها ومعتقداتها والترويج لدعايتها التي يمكن أن تؤسس إلى فكر تكفيري[55].

- ازدياد الهجمات الالكترونية (Cuber attacks) على المواقع الحساسة والبنى التحية الحيوية، مما قد يلحق خسائر مالية معتبرة للدولة (في سنة 1995أصبح البنك البريطاني خارج نطاق العمل، في سنة 2008 خسر البنك الفرنسي أكثر من ستة (06) مليار يورو، في عام 2011 خسر البنك السويسري (02) مليار دولار)[56].

- تضاعف عمليات الانتحال الشخصي والرسمي لعدد من واجهات وصفحات التواصل الاجتماعي، وتزايد عمليات الابتزاز الناجمة عن اختراقات الأنظمة والمواقع للحصول على أموال غير مشروعة، أو الحاق الأذى بأصحابها[57].

- الهجمات على مرافق الأمن والدفاع الوطني التي تعتبر مرافق جد حساسة وحيوية نظرا لإتصالها بالوجود الأساسي للدولة وحماية كيانها من مختلف أشكال الإختراق، فأصبح الحديث اليوم عن هجمات الجيوش الإلكترونية النشطة في العديد من الدول، وإمكانياتها على إصابة القدرات الدفاعية والهجومية للدول. ففي هذا

الخصوص، حذر وزير الدفاع الأمريكي السابق **ليون بانيتا** من إمكانية تعرض الولايات المتحدة الأمريكية لهجمات إلكترونية شرسة تفوق مستوى خسائرها وأضرارها بكثير الهجوم الياباني على قاعدة بيرل هاربر في أثناء الحرب العالمية الثانية، مع مخاطر زيادة إرباك شبكات الكهرباء، المواصلات، البنى التحتية، المواقع الحكومية تعطيل حركة القطارات...[58].

- تعريض الأمن القومي والدفاع الوطني للدول لمزيد من الانكشافات والتهديدات الخارجية، خاصة في ظل الحديث على ظاهرة "الجيوش الالكترونية" النشطة في العديد من دول العالم، وما تنطوي عليه من مخاطر عالية على أمن الدول من حيث سرعة قدراتها الهجومية الموجودة أو تلك التي يجري تطويرها، الأمر الذي استدعى الجنرال الأمريكي كيلر (R.KEHLER) من القيادة العسكرية للولايات المتحدة الأمريكية في سنة 2011 المخاطبة قائلا: "... نحن بحاجة الى تحديد قواعد الاشتباك لحرب الحواسب الهجومية"[59].

- صناعة ونشر الفيروسات التي تعتبر الأكثر إنتشارا على الصعيد الأمن المعلوماتي، والتي من شأنها إحداث أضرار إلكترونية بليغة، قد تمس الأمن العام في البلد، من خلال حذف المعلومات وقرصنتها، إحداث بلبلة وخسائر إقتصادية ومادية جسيمة، من شأنها شل وإضعاف المؤسسات العامة في الدولة[60].

من جانبه، نجد أنه من بين أهم التحديات التي باتت تطرحها العولمة في عالمنا المعاصر اليوم تتمثل أساسا فيما يصطلح على تسميته "بالحروب السيبرانية" من حيث كونها تهديدات جديدة على الأمن القومي للدول، خاصة ما تشهده بعض دول العالم من هجمات الكترونية وعمليات قرصنة تطال أنظمتها الحيوية ومنشآتها الاستراتيجية (ففي سنة 2010 تم اكتشاف الفيروس الإسرائيلي " Stuxnet" المسؤول عن تخريب وتعطيلأنظمة وبرامج الحواسيب التابعة لمحطة الطاقة النووية في مدينة بوشهر الإيرانية. كذلك نجد تسريبات العميل الاستخباراتي الأمريكي السابق ادوارد سنودن (الموظف السابق في وكالة الأمن القومي NSA) لسنة 2013 التي مفادها قيام الحكومتان الأمريكية وحليفتها البريطانية بتنفيذ مخططات تجسسيةسيبرانية شاملة)[61].

الخلاصة:

في ختام هذه الدراسة، التي حاولنا عبرها تسليط الضوء على أحد أهم التهديدات التي باتت تواجهها الدول اليوم، والمتمثلة في الجرائم الإلكترونية المستفحلة النشاط بفعل الإستخدامات المكثفة لأجهزة الإتصالاتالحديثة وسرعة الوصول إلى المعلومة بأسهل الطرق الممكنة.حيث أن هذه الجرائم المستحدثة الناتجة عن تطور تقنية نظم المعلومات ما هي إلا إنعكاس مباشر لثو رة التكنولوجيا الرقمية، وشكل من أشكال الإساءة المقصودة من الجناة لثورة نظم المعلومات، سواء أكان فعل الجاني لإظهار قدراته وإمكاناته التقنية العالية، أم كانت لديه الميول الإجرامية الظاهرة أو الخفية، والتي يسعى منها إلى تحقيق مكاسب غير مشروعة له أو لغيره، وهو ما يعرض أمن

الأشخاص والدول إلى العديد من المخاطر والتهديدات الناجمة عن تلك الهجمات التي تستهدف أنظمة وبيانات الأجهزة الرسمية والخاصة في الدولة.

لذا، فقد أفرز التطور العلمي والتكنولوجي الذي يعد أحد مظاهر العصر الحديث، ثورة في الإتصالات والمعلومات، ساعدت البشرية على تخطي العديد من العراقيل والحواجز التي كانت تعترضها في السابق، وبالتالي فقد فتحت المجال لآفاق تقدم ورقي الحضارة الإنسانية في مختلف المجالات جراء ما توفره من خدمات وتسهيلات بغية تحقيق أرقى مستوى للحياة البشرية.لكن في الوقت نفسه،فإن هذا التطور التكنولوجي والعلمي الهائل في الإتصالات والمعلومات خلق بدوره وضعا جديدا يحمل في طياته تهديدات جمة وعلى مختلف الأصعدة، أصبح يتعرض لها العامل البشري والحكومات والمنظمات...، بحيث أفرزت الإستخدامات غير المسؤولة من قبل البعض لثورة المعلومات، العديد من السلوكيات الضارة بقيم وحقوق وأمن الشعوب والدول، وبالتالي، فقد أضحت هذه الأخيرة في وضعية تهديد شديد ومستمر غير مسبوق.

الاحالات و قائمة المراجع:

1- طارق إبراهيم الدسوقي عطية، **الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية (**الاسكندرية: دار الجامعة الجديدة للنشر، 2009)، ص.12.

2- غنية باطلي، **الجريمة الالكترونية: دراسة مقارنة** (الجزائر: الدار الجزائرية للنشر والتوزيع، طبعة 2016)، ص.5.

3- أشرف السعيد أحمد، **استراتيجية أمن المعلومات** (مصر: ب د ن، ط1، 2014)، ص.49.

4- عبد الرحمان شعبان عطيات، **أمن الوثائق والمعلومات** (الأردن: **الأكاديميون للنشر والتوزيع؛ دار حامد للنشر والتوزيع، ط1، 2014)، ص ص.121،122.**

5- جلال محمد الزعبي وأسامة أحمد المناعسة، **جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة**(الأردن: دار الثقافة للنشر والتوزيع، ط1، 2010)، ص.62.

6- المرجع نفسه، ص.63.

7- طارق إبراهيم الدسوقي عطية، مرجع سابق، ص.169.

8- غنية باطلي، مرجع سابق، ص. 7.

9- طارق إبراهيم الدسوقي عطية، مرجع سابق، 169.

10- جلال محمد الزعبي وأسامة أحمد المناعسة، مرجع سابق،ص.64.

11-طارق إبراهيم الدسوقي عطية، مرجع سابق، ص.143.

12-أمير فرج يوسف، **الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكومبيوتر والأنترنت** (الإسكندرية: مكتبة الوفاء القانونية، ط1، 2011)، ص.63.

13-أحمد عبد الرحمن المجالي، "الظواهر الإجرامية الحديثة والجريمة المنظمة"، **مجلة العلوم الإنسانية**، ع32، جامعة محمد خيضر بسكرة، (نوفمبر 2013)، ص.226.

14-خالد ممدوح إبراهيم، **الجرائم المعلوماتية** (الإسكندرية: دار الفكر الجامعي، ط1، 2009)، ص.21.

15-المرجع نفسه، ص.74.

16-أمير فرج يوسف، **الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكومبيوتر والأنترنت** (الإسكندرية: مكتبة الوفاء القانونية، ط1، 2011)، ص.10.

17- Solange Ghernaouti-Hélie, **La cybercriminalité : le visible et l'invisible** (Lausanne : Collection Le Savoir Suisse, 1re édition, 20009), p.14.

18-طارق إبراهيم الدسوقي عطية، مرجع سابق، ص.151.

19-غنية باطلي، مرجع سابق، ص.15.

20- طارق إبراهيم الدسوقي، عطية، مرجع سابق، ص.158،157.

21- Miryam QUEMENER et Yevs CHARPENEL, **Cybercriminalité : droit pénal appliqué** (Pris : Economica, 2010),p.8.

22-أحمد عبد الرحمان المحالي، مرجع سابق، ص.227

23-أمير فرج يوسف، مرجع سابق، ص ص.11،12.

24-غنية باطلي، مرجع سابق، ص ص.25-32.

25-*(يعتبر الكاتب وليام غبسونWiliam GIBSON هو من أطلق مصطلح الفضاء السيبرياني - Cyberespace- سنة 1984 في مؤلفه المسمى Neuromancer).أنظر: Miryam QUEMENER et Yevs CHARPENEL, **Cybercriminalité : droit pénal** appliqué (Pris :Economica,2010),p.7.

26-خالد ممدوح إبراهيم، **الجرائم المعلوماتية**، الإسكندرية: دار الفكر الجامعي، ط1، 2009، ص ص.76-86.

27- غنية باطلي، مرجع سابق، ص.34.

28-المرجع نفسه، ص.51.

29-أمير فرج يوسف، مرجع سابق، ص. 17.

30-محمد عبد الحسين الطائي وينال محمود الكيلاني، **ادارة أمن المعلومات** (الأردن: دار الثقافة للنشر والتوزيع، ط1، 2015)، ص.16.

31-جلال محمد الزغبي وأسامة أحمد المناعسة، **جرائم تقنية نظم المعلومات الالكترونية: دراسة مقارنة** (عمان: دار الثقافة للنشر والتوزيع، ط1، 2010)، ص ص.107-209.

32-جلال محمد الزعبي وأسامة أحمد المناعسة، مرجع سابق، ص. 135.

33- Enjeux et difficultés de la lutte contre la "dans : cybercriminalité:www.inhesj.fr/sites/default/files/files/formation/gds6.**pdf**

34- www.un.org/french/events/10thcongress/2088hf.htm

35- Miryam QUEMENER et Yevs CHARPENEL, **Cybercriminalité : droit pénal appliqué** (Pris :Economica,2010), p.132.

36- جلال محمد الزغبي وأسامة أحمد المناعسة، **جرائم تقنية نظم المعلومات الالكترونية: دراسة مقارنة** (عمان: دار الثقافة للنشر والتوزيع، ط1، 2010)، ص. 155.

37- المرجع نفسه، ص. 164.

38- جلال محمد الزعبي وأسامة أحمد المناعسة، مرجع سابق، ص. 197.

39- عبد الرحمان شعبان عطيات، **أمن الوثائق والمعلومات** (الأردن: **الأكاديميون للنشر والتوزيع؛ دار حامد للنشر والتوزيع، ط1، 2014)، ص ص.79،80.**

40- www.unodc.org/...EG.../UNODC_CCPCJ_EG4_2013_2_F.**pdf**

41- جلال محمد الزغبي وأسامة أحمد المناعسة، مرجع سابق، ص. 222-272.

42- خالد بن سليمان الغثبر ومحمد بن عبد الله القحطاني، **أمن المعلومات (**المملكةالعربية السعودية: مكتبة الملك فهد الوطنية، 2008)، ص.20.

43- Miryam QUEMENER et Joël FERRY, **Cybercriminalité : défi mondial** (Pris :Economica, 2me édition, 2009),p.150.

44- Miryam QUEMENER et Joël FERRY, op.cit**,** p.96.

45- يوسف صغير، " الجريمة المرتكبة عبر الأنترنت"، مذكرة ماجستير غير منشورة، الجزائر: جامعة تيزي وزو، 2013.ص.54.

46- محمد علي حيدر، **مختصر الدراسات الأمنية**(الرياض: المركز العربي للدراسات الأمنية والتدريب، 1993)، ص. 34.

47- خالد ممدوح إبراهيم، مرجع سابق، ص.393.

48- عصمت عدلي، **الإعلام الأمني بين النظرية والتطبيق** (الإسكندرية: دار الجامعة الجديدة،2011)، ص.19.

49- محمد عبد الحسين الطائي وينال محمود الكيلاني، **إدارة أمن المعلومات** (الأردن: دار الثقافة للنشر والتوزيع، ط1، 2015)، ص.37.

50- أشرف السعيد أحمد، **استراتيجية أمن المعلومات** (مصر: ب د ن، ط1، 2014)، ص ص.110،111.

51- محمد عبد الحسين الطائي وينال محمود الكيلاني، مرجع سابق، ص.36.

52- Solange GHERNAOUT-HELIE, op. cit. p.28.

53- محمد عبد الحسين الطائي وينال محمود الكيلاني، مرجع سابق، ص.47.

54- جمال العيفة،" صناعة البرمجيات، الثروة المنسية" في،**المجلة العربية الدولية للمعلوماتية**(العربية السعودية: جامعة نايف للعلوم الأمنية، العدد 5، مجلد 3) (جانفي 2011)، ص.70.

55- محمود شاكر سعيد وخالد بن عبد العزيز الحرفش، **مفاهيم أمنية** (المملكة العربية السعودية: جامعة نايف العربية للعلوم الأمنية، ط1، 2010)، ص.75.

56- محمد عبد الحسين الطائي وينال محمود الكيلاني، مرجع سابق، ص ص.21،22.

57- المرجع نفسه، ص ص.22،23.

58- جمال سند السويدي، **وسائل التواصل الاجتماعي ودورها في التحولات المستقبلية: من القبيلة إلى الفايسبوك**، (الإمارات العربية المتحدة: مركز الإمارات للدراسات والبحوث الإستراتجية، ط4، 2014)، ص.100.

59- محمد عبد الحسين الطائي وينال محمود الكيلاني، مرجع سابق، ص ص.47،48.

60- محمود شاكر سعيد وخالد بن عبد العزيز الحرفش، مرجع سابق، ص ص.75،76.

61- عبد العزيز جراد، **الجيوسياسية: مفاهيم، معالم ورهانات** (الجزائر: منشورات الشيهاب، 2012)، ص.127.